

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
19 mai 2005 (19.05.2005)

PCT

(10) Numéro de publication internationale
WO 2005/046278 A2

(51) Classification internationale des brevets⁷ : **H04Q 7/38**

(21) Numéro de la demande internationale :
PCT/EP2004/052773

(22) Date de dépôt international :
3 novembre 2004 (03.11.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03104069.4 4 novembre 2003 (04.11.2003) EP

(71) Déposants (pour tous les États désignés sauf US) :
NAGRACARD S.A. [CH/CH]; Route de Genève 22,

CH-1033 Cheseaux-sur-Lausanne (CH). SWISSCOM
MOBILE AG [CH/CH]; Schwarztörstrasse 61, CH-3050
Berne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : KSON-
TINI, Rached [CH/CH]; Route Aloys Fauquez 26,
CH-1004 Lausanne (CH). CANTINI, Renato [IT/CH];
Route du Moulin 35, CH-1782 Belfaux (CH).

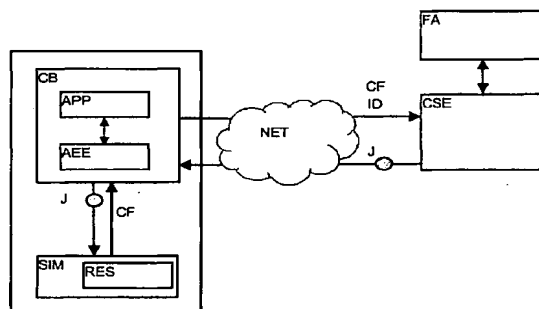
(74) Mandataire : WENGER, Joel; Léman Consulting S.A.,
Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,

[Suite sur la page suivante]

(54) Title: METHOD FOR MANAGING THE SECURITY OF APPLICATIONS WITH A SECURITY MODULE

(54) Titre : MÉTHODE DE GESTION DE LA SÉCURITÉ D'APPLICATIONS AVEC UN MODULE DE SÉCURITÉ



(57) Abstract: The aim of the invention is a method for managing the security of the assembly of equipment, security module and applications, with the aim of reducing the risks associated with the possible use of a security module with bad intentions, by applications executed on a type of equipment and/or a software version not entirely meeting the established security criteria. Said aim is achieved, by means of a method for managing the security of applications (APP), functioning in a piece of equipment (CB), connected to a network (NET), said network (NET) being administered by a control server (CSE) of an operator, said applications using resources (RES) (data or functions), stored in a security module (SIM), connected locally to said equipment (CB), comprising the following preliminary steps: receipt of data comprising at least the type and the version of the equipment software (CB) and the identity of the security module (SIM), over the network by the control server, analysis and verification by the control server (CSE) of said data (ID), generation of a cryptogramme (J), from the result of the verification of said data (ID), and transmission of said cryptogramme (J), by means of the network (NET) and the equipment (CB), to the security module (SIM). Said method is characterised in that the security module (SIM) analyses the cryptogramme (J) received and activates and deactivates, respectively, resources (RES) (data or functions), used by at least one application (APP), installed in the equipment (CB), said cryptogramme (J) comprising instructions changing the function of the application (APP) according to criteria established by the application provider and/or the operator and/or the equipment user.

(57) Abrégé : Le but de la présente invention est de proposer une méthode de gestion de la sécurité de l'ensemble équipement, module de sécurité, applications afin de limiter les risques liés au fait qu'un module de sécurité soit utilisé à mauvais escient par des applications exécutées sur un équipement de type et/ou de version de logiciel ne remplissant pas entièrement les critères

[Suite sur la page suivante]



GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

- (84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE,

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

de sécurité établis. Ce but est atteint par une méthode de gestion de la sécurité d'applications (APP) fonctionnant dans un équipement (CB) connecté à un réseau (NET), ledit réseau (NET) étant administré par un serveur de contrôle (CSE) d'un opérateur, lesdites applications utilisant des ressources (RES) (données ou fonctions) stockées dans un module de sécurité (SIM) relié localement audit équipement (CB), comprenant les étapes préliminaires suivantes: réception de données comprenant au moins le type et la version de logiciel de l'équipement (CB) et l'identité du module de sécurité (SIM), via le réseau, par le serveur de contrôle ; analyse et vérification par le serveur de contrôle (CSE) desdites données (ID); génération d'un cryptogramme (J) à partir du résultat de la vérification sur lesdites données (ID), et transmission dudit cryptogramme (J), via le réseau (NET) et l'équipement (CB), au module de sécurité (SIM), ladite méthode est caractérisée en ce que le module de sécurité (SIM) analyse le cryptogramme (J) reçu et active, respectivement désactive des ressources (RES) (données ou fonctions) utilisées par au moins une application (APP) installée dans l'équipement (CB), ledit cryptogramme (J) comprenant des instructions conditionnant le fonctionnement de l'application (APP) selon des critères établis par le fournisseur de ladite application et/ou l'opérateur et/ou l'utilisateur de l'équipement.